UiO : Faculty of Law
University of Oslo

The Applicable Law to the Electronic Contracts under EU Data Protection Directive

Directive perspective – extended territorial scope

Candidate number: 8011

Supervisor: Olga Mironenko Enerstvedt

Submission deadline: 1.12.2013

Number of words: 17 349

1 Introduction

1.1 The Importance of the Thesis and Actuality of the Chosen Topic

The technological development and new achievements in internet-globalized world avail the business of possibility to offer online service to the customers/user[1] and form electronic contract on internet. Such contracts raise number of legal questions as to the legal framework applicable thereto. First and the most significant factor is that there is no precise doctrine on internet regulation. This issue is under debated and still is a question of an authority controlling the behavior of actors on the internet. For example, Lessig considers that internet should be self-regulated sphere,[2] whereas Froomkin thinks the model of internet regulation contains the element of government interfere.[3] Hence, the issue on internet regulation is open for debate, which enables the business to freely define the rules they consider appropriate in electronic contracts.

The dominant position of the business on internet market is based on "take it or leave it" approach.[4] This empowers the business to make one-sided rules and decide the terms for the electronic contract[5] without permitting users/customers to alter, amend or delete clauses of the electronic contract. If the customer does not agree with the terms offered in electronic contract, has no possibility to change them and must either accept or reject the service.

[1] I am using word "customer/user" in the same context. In the text you can find either of them and they have the same meaning.
[2] for the further issues see, Lessig, *Code*. Lessig considered that the cyberspace is self-regulated sphere.
[3] for the further issues see Froomkin, "Almost Free: An Analysis of ICANN's 'Affirmation of Commitments.'"
[4] Bender, "Privacy in the Cloud Fronter: Abandoning the 'Take It or Leave It' Approach," 500–501.
[5] see decision Gatton v. T-Mobile USA, Inc., the California Court of Appeals 61 Cal. Rptr. 3d 344, 356–58 (Cal. Ct. App. 2007), cert. denied, 553 U.S. 1067 (2008). (n.d.).

Further, while entering into electronic contract users rarely ever realize that they disclose their privacy to the unknown number of the business representatives (head office of the company, subsidiaries, or branch offices). Moreover, they are not aware that business offers cloud service to them[6] and by clicking on a button "accept", they share private information to the cloud service providers.[7] Regarding the said provisions there always is a legitimate fair of misuse of user's private data: where does the data uploaded in electronic contracts go through the cloud service? Who has an access to such data? Is it only the service provider that acquires such information or is it also disclosed to other parties, especially in the conditions, when we upload our financial information, bank account number to the internet? What is the law governing the above legal questions?

These are the difficulties which we face when entering into electronic contract and share our private information. Customers may be under fair give access bank account number to the cloud computing service providers. What should be the way out of the situation? – Relevant legislation on data protection – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "Directive"), its scope for the protection of European citizen's data.

European data protection directive defines the circumstances when European law should be applied, because it is considered that the standard of the directive is appropriate to the purpose - protect data of the citizens. At the same time directive guarantees enough high level of protection to the European citizen's data. Therefore, the main aim of the directive could be to cover, not the surface of the data protection platform but also the content of the internet, control misuse of user's data. Significant point is the territorial scope of application of the EU law for the protection of EU citizen's data, discuss in more details below in this thesis.

---

[6] Bender, "Privacy in the Cloud Fronter: Abandoning the 'Take It or Leave It' Approach," 511–512.

[7] Bradshaw, Millard, and Walden, "Contracts for Clouds," 191. According to the article, "'Provider' is the business organization that offers the cloud service, whilst a 'Service' is the particular cloud service in question"

1.2 The Research Question of the Thesis

The foregoing study is mainly focused on companies/service providers[8] established within the EU. The thesis is limited to defining applicable law criteria according to the European data protection directive, Article 4 (1) (a) and (c).

As a starting point, this study will analyze whether the EU law applies in every case when the user/customer enters into electronic contract with the EU established business/service provider. The question itself calls for identifying the applicable law to the EU established companies. The study evaluates the requirements of the law and to what extent the law is clear enough or whether it contains theoretical provisions which will not work in practice. Also the study identifies to what extent are the contractual choice of law clauses mandatory in electronic contracts, or whether EU directive provisions or consumer protection rules can not be overridden by such choice.

The study further analyzes Articles 4 (1) (a) and (c) of the EU Directive to identify to what extent the provisions cover non-EU established companies thereby establishing extra-territorial outreach of EU rules. I would like to mention that question is not connected to the directive article 25 and 26. Considering subject matter of the article 25 and 26 they deal with non-EU established companies, which have no direct business connection to the European data protection market. The EU Directive requires adequate protection of the data while customer's information flows to the non-EU established companies. Therefore, the thesis will focus on companies which have connection to the European market for the purposes of Article 4 (1) (a) and (c), such as either the EU establishment of the company, or processing of data for the context of the EU establishment or use of EU equipment by the company to transfer data.

[8] In the thesis when it is mentioned "Company", "Service Provider" "Cloud Service Provider" "Website" they have the same meaning.

1.3 Method of the Research and Sources

The approach of the master thesis is theoretical legal research methodology. The main aim of the thesis is to analyze how article of applicable law of data protection directive works in practice. For the said purpose I am giving examples from the websites and court cases on showing dynamic approach on applicable law.

The study is primarily based on the EU Directive, which this thesis seeks to analyze within the scope of its subject matter. The study also analyzes provisions from the new regulation - Proposal for a Regulation of the European Parliament and of the Council-on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "Data Protection Regulation" or "Regulation") which will enter into force by the beginning of 2015.[9] It is important to notice that every time I will mention regulation, I mean LIBE committee's amended version of regulation 21 October, 2013, as of the date hereof.[10]

As a secondary source, the study relies on opinions of Article 29 data protection working party. According to Article 29 of the data protection directive working party prepares recommendation and mostly interpret the provisions of the directive. Non-binding nature of such recommendations does not weaken their authoritative power. In fact, the number of recommendations increases gradually and they are largely followed by organizations when dealing with data protection issues.[11] Therefore, recommendations issued by working group are certainly one of the most important sources for interpretation of articles of the data protection directive.

Further, practical examples will be analyzed to better obviate how the law works in practice. Precisely, two websites, www.booking.com and www.hostelworld.com will be

[9] Final report to the Information Commissioner's Office, *Implications of the European Commission's Proposal for a General Data Protection Regulation for Business*, p 13.
[10] see link here :http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131021_1830.htm
[11] Poullet, "EU Data Protection Policy. The Directive 95/46/EC," 208. Wong, "Data Protection," 53–54.

analyzed as examples of cloud computing services, which enter into electronic contract with the users for rendering hotel-booking service. These websites are established in EU and that's why examples are appropriate to the subject matter of the thesis – defining applicable law in electronic contracts.

And last but not least, the study further relies on and discusses the most important court decisions on the relevant provisions of the Directive. The aim is to find a common line of reasoning applied by European courts when dealing with the subject matter.

1.4 Structure of the Thesis

The first chapter of the thesis is introduction, which contains the explanation why the topic was chosen, the approach of the thesis – what legal questions thesis will answer.
The second chapter deals with the issue on explanation what electronic contract is to the connection between e-contract and cloud computing service. Also the chapter will make clear functions of user and service provider in electronic contract, will be shown counterarguments what benefit has considering user as a controller or data subject? If the service provider's status of processor is appropriate to the function.
The third chapter firstly gives the general criteria of applicable law, later on explains the problems which should be raised in practice while defining choice of law in electronic contracts.
Chapter 4 will finalize the conclusion of the thesis.

2 Legal Elements for the Processing of Data in Electronic Contracts: Who is Doing What?

This chapter introduces the legal nature of electronic contract, what does it cover, contract between service provider and user? It is considered that they enter into electronic contract. Regarding that fact I will try to explain what I mean under electronic contracts. How is connected electronic contract to cloud computing service.

Further, the role and legal functions of users and service providers are of particular importance when discussing electronic contracts. Therefore, this chapter seeks to establish the functional scope of the parties to the electronic contracts. Particular emphasis will be placed on the controversial ideas regarding the party functioning as the controller in the clouds. It is the controller who has to take responsibility and give directions on the processor to handle processing in the clouds. The chapter seeks to identify whether the requirements under the law in fact coincide with the reality: who controls data and who processes it? The said subchapter will be guide for the future defining applicable law, as controller and processor plays important role considering EU law is applicable in European established companies or not.

After becoming clear the role of user and the service provider I should define what information user processes on the website, if information falls under the concept of the personal data. As a last concern, the chapter will discuss whether the type of information that user processes on the website can fall under the concept of the personal data.

2.1 The Legal Aspect of Electronic Contract

2.1.1 Definition of Electronic Contract

There is no comprehensive definition of electronic contract provided in legislation. Nevertheless, the possibility to enter into contract by using "electronic means" is expressly acknowledged by Article 9 "Directive of European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market" ('Directive on electronic commerce').[12] The same provision can be found in the Directive of the European Parliament and of the Council on the protection of consumers in respect of distance contracts – ("Distance selling directive") which avails the parties of possibility to form a contract "by means of one or more distance communication."[13] The said definitions propose that electronic contract is qualified as an agreement between service provider and the user, which is "operated by electronic means"[14] in the internet. Both directives refer to "electronic means", which is the main feature for considering a contract to be electronic one. The wording "electronic means" is electronic equipment, which is used by the parties to enter into the agreement.[15] At the same time Electronic contract consists from the "programming, language syntax "checkable interfaces (or services)" which are necessary for the software to work with electronic equipment.[16] The electronic equipment is the program, which represents service provider and users by accepting conditions and rules online enter into electronic contract.[17]

Interesting point is that electronic commerce directive leaves the choice to the Member States to decide themselves, under their national legislation, as to when the offer or acceptance is

[12] "Directive 2000/31/EC."
[13] "Directive 97/7/EC," article 2 (1).
[14] "Directive 2000/31/EC," article 9.
[15] Ibid., Recital 17–18.
[16] Nuth, "E-Commerce Contracting: The Effective Formation of Online Contracts," 43–44.
[17] Weitzenboeck, "Electronic Agents and the Formation of Contracts," section 1.2.

formed and contract is concluded.[18] The directive thus, only provides a legal framework for a possibility to negotiate by using electronic means.

Usually, in electronic contracts, consumers follow three-step procedure.[19] Mostly, in terms and conditions of the electronic contracts providing information about the service, the location of the hotel, conditions of the contract suggested by service provider is an invitation to treat.[20] The user makes offer when agrees the terms and conditions of the contract. After receiving the confirmation latter from the service provider, as accept, it is the settled contract between parties.[21]

The important factor is to mention that parties of the electronic contract are service provider and the user. The research focusing on electronic contract, where user\customer agrees on terms and conditions suggested by service provider, this type of contract is considered as click-wrap contract.[22] The question could be online service, such as book hotel and agreement on standard contractual rule is considered as electronic contract or not? According to the definition of electronic contracts, online service, such as book hotel is electronic contract. Because users, by electronic mean/program accepting the rules suggested by the service provider.[23] The operation of accept contractual terms without any possibility of alter, amend or delete is standard contractual rule.

[18] Winn, J.K. & Haubold, J., "Electronic Promises: Contract Law Reform and E-Commerce in a Comparative Perspective," 12.
[19] Ramberg, C.H, "The E-Commerce Directive and Formation of Contract in a Comparative Perspective," 14.
[20] *Law and the Internet*, 103.
[21] Ramberg, C.H, "The E-Commerce Directive and Formation of Contract in a Comparative Perspective," 14.
[22] Boss, "IV. Electronic Contracting: Legal Problem or Legal Solution?," 129–130. Davidson, *The Law of Electronic Commerce*, 68.
[23] Zimmeck, "The Information Privacy Law of Web Applications and Cloud Computing," 453–454.

2.1.2 Electronic Contract as a Cloud Service?

The previous section explained the essence of an electronic contract, where a user/consumer is in interaction with a service provider.[24] This part of the study defines the types of online services offered by the service provider in electronic contract. The ultimate aim is to identify whether such services can qualify as cloud services offered to the users. This however can be achieved by defining the term "cloud computing" in the first place.

The cloud computing is considered as *"storing, processing and use of data on remotely located computers accessed over the internet"*[25]. The most popular and reasonable definition of cloud computing is given to the US National Institute of Standards and Technology (NIST) which states that "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*[26].

In case of electronic contracts, service providers should be considered as cloud service providers at the same time.[27] As suggested by the definition of the cloud computing, service providers render shared service offered by computer program.[28] For the purposes of this study, the service provider is a business organization, which offers public service to the users. Service, such as booking a hotel online, is offered and addressed to the unlimited number of

[24] Nuth, "E-Commerce Contracting: The Effective Formation of Online Contracts," 43–44.
[25] "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions 'Unleashing the Potential of Cloud Computing in Europe,'" 2.
[26] US NIST SP 800-145, The NIST Definition of Cloud Computing, Sept. 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[27] In these articles you can see full definition of cloud computing as well. Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 4–5; Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 3–4., Hon and Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4," 4–5; 14., Bradshaw, Millard, and Walden, "Contracts for Clouds," 187–191.Hon, Millard, and Walden, "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now," 82–83; 103., "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe,'" 4–5. Gutwirth, Computers, Privacy and Data Protection an Element of Choice, 381.
[28] Bender, "Privacy in the Cloud Fronter: Abandoning the 'Take It or Leave It' Approach," 497.

users in online website. It should be considered that according to the said assertion service provider is using public cloud[29] and shares the service in the internet with the users. Business could be using Software as a Service (hereinafter "SaaS") infrastructure and giving possibility to the users, from the different part of the world enter into contract and share public cloud.

When speaking of the electronic contracts, as the cloud computing service, one should be mindful of the fact that, according to the terms and conditions of the service providers,[30] users enter into contract with the hotel owner when booking the hotel. The service provider is merely an intermediary between the user and the owner of the hotel facility. From the point of view of the service provider policy, there is no direct legal relationship between service provider, on the one hand, and the user, on the other hand. In other words, the service provider has no binding legal obligations towards the user/client. However, does the same apply in reality with respect to cloud computing services?

Usually, in cloud computing scenario, users and service providers enter into contract, which can be of two types: paid service contract and unpaid service contract.[31] With respect to hotel booking services, website's policy defines that it is not a paid service and website has no commercial interest in it.[32]

[29] Detailed description of public loud and SaaS service see in the following sources. Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 4–5; Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 3–4., Hon and Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4," 4–5; 14., Bradshaw, Millard, and Walden, "Contracts for Clouds," 187–191.Hon, Millard, and Walden, "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now," 82–83; 103., "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe,'" 4–5. Gutwirth, Computers, Privacy and Data Protection an Element of Choice, 381.

[30] http://www.booking.com/general.en-gb.html?dcid=1&lang=en gb&sid=ecabfd4cd95f5afa3f2080bd637e9437&tmpl=docs%2Fterms-and-conditions; http://www.hostelworld.com/hosteltermsandconditions.php

[31] Bradshaw, Millard, and Walden, "Contracts for Clouds," 196–197.

[32] http://www.booking.com/general.en-gb.html?dcid=1&lang=en gb&sid=ecabfd4cd95f5afa3f2080bd637e9437&tmpl=docs%2Fterms-and-conditions; http://www.hostelworld.com/hosteltermsandconditions.php

However, in case of providing cloud computing service, one should distinguish between: the contracts with the service provider, where they are free to define the terms of the agreement unilaterally, on the one hand, and statutory regulations on privacy issues, data protection directive, national rules, on the other hand.[33] The important assertion is that, while there is a contract between parties, it does not necessarily mean that the contract is self-sufficient and mandatory provisions of law can be overridden altogether. Even if the valid contract exists, the statutory regulations may still be applicable and binding for the parties.[34] However, Contractual rules and conditions on the website do not necessarily mean that rules are according to the data protection directive.[35]

Cloud service providers are the party of the contracts entered into between the users and the ultimate contractor, which renders the services purchased online, such as owners of the hotel facilities in the case at hand. They enter into electronic contract with the user, suggesting online service and undertake responsibility to protect user's data from disclosure.[36] Service provider could be held liable if third person has access to personal data.[37] However, as cloud service provider, the website is obliged to follow data protection directive. With the same token, merely a contractual provisions exempting the service provider from liability by outlining that the service provider is merely an intermediary between parties and is free from the obligation, may not be relied upon with respect to misuse of personal data. Service providers must therefore comply with the mandatory rules on data protection.

---

[33] Zimmeck, "The Information Privacy Law of Web Applications and Cloud Computing," 465.
[34] Ibid. Bradshaw, Millard, and Walden, "Contracts for Clouds," 195–196.
[35] Hon, Millard, and Walden, "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now," 98–103.;
[36] in case of booking com: "Your privacy is important to us. We value the trust you have placed in us, and are committed to protecting and safeguarding any personal information you give us. " in case of hostelworld.com: "Hostelworld.com and its associated companies respect and protect your right to privacy in relation to your interactions with this website. Any information which is provided by you to Hostelworld.com via this website or otherwise will be treated in accordance with the terms of the Irish Data Protection Acts, 1988 and 2003 and/or such amending or replacement legislation as may be adopted in Ireland from time to time."
Gutwirth, *Computers, Privacy and Data Protection an Element of Choice*, 348. usually service providers guarantee the security of the data.
[37] "Directive 95/46/EC," article 7 (a).

To sum up, the available definitions of electronic contract leaves the room for the argument that the implied contract is entered into between the cloud service provider and the user. Therefore, service providers have the right to protect data of the users and not to give access thereto to third parties. At the same time, service providers contracting terms are legally binding but it does not necessarily mean that law should not be a regulator at the same time. Contractual terms, which go against the mandatory rules of law may not be considered legally valid and enforceable. Having said this, it is now clear that the relationship between the parties to electronic contract is not completely detached from the applicable law and left to autonomous regulation under the contractual terms. The law applicable to such relationship is of outmost importance when identifying legal rights and obligations of the parties to the electronic contract. Therefore, the study will further discuss in details how the data protection rules effect electronic contracts and override contractual terms with respect to the function and responsibility of the parties.

2.2 Parties of the Electronic Contract

2.2.1 Two Tier Role of the User in Electronic Contract: Controller or Data Subject?

The user is the main party to the cloud computing service during the electronic contracting. Should user be qualified as a controller according to the data protection directive? To answer to this question, one should analyze the definition of controller. Identification of the controller is essential for determining the applicable law.[38]

[38] Bygrave, "Determining Applicable Law pursuant to European Data Protection Legislation," 4. "Article 29 Data Protection Working Party, WP 179," 8.

The data protection directive[39], as the data protection regulation[40] gives definition of controller and considers that controller can be a natural or a legal person, who "determines the purposes and means of processing of personal data".[41]

It should be mentioned that controller is the person who processes data according to the law adopted by the state. However, this provision does not require that controller should be appointed by any legal body or the institution and should fulfill their directions. Controller should regulate data processing issues without any special appointment by law and should be independent from the governmental power.[42] That means that the controller should not be only administrative body, but any other legal entity or individual person. The main idea of the data protection directive is to form easy procedure to define controller. That's why directive gives the possibility to the natural person, without any governmental supervision control the data of the users. On this issue counter idea has Article 29 data protection working party. They consider that data controller should not be a natural person, because legal person or organization could effectively fulfill obligation rather than natural person.[43] However, the presumption of consider natural person as a data controller is not appropriate to the directive provisions. Data protection gives possibility not only one person to be a controller, but several controllers to process data jointly.[44]

Another key element about the controller is the purpose of the processing: if the natural person, or the legal body had the purpose to process data and at the same time was initiator of processing.[45] This means that the data must be collected on the specified legitimate purpose and processed only for the said reason, not used for the other circumstances[46]. This provision

[39] "Directive 95/46/EC," article 2 (d).
[40] "Commission Proposal COM(2012) 11 Final 2012/0011 (COD) C7-0025/12," article 4.5.
[41] "Directive 95/46/EC," article 2 (d).
[42] "Article 29 Data Protection Working Party, WP 169," 8.
[43] Ibid., 15.
[44] Bygrave, "Determining Applicable Law pursuant to European Data Protection Legislation," 8.Moerel, "Back to Basics," 7–8.
[45] "Article 29 Data Protection Working Party, WP 169," 12–14.
[46] Ibid., 8–9.;

is linked to the controller's responsibility lawfully process data[47] and not to disclose it to the third parties without due consent to the data subject.

In cloud computing service user is considered as a data controller.[48] To analyze formal requirements of controller, there is no doubt that user makes independent decision when processes data to the cloud computing service. At the same time the criteria of "initiator of the processing" is complied and user gives direction to the service provider where the data should be sent, orders service/hotel in EU territory or outside EU territory.[49]

Although, there should be several question how user could fulfill the obligation of controller. Firstly, user is not participating in forming standard contractual rules and accepts suggested rules of service provider.[50] This fact weakens the user's function as a controller and decreases the power of the controller to my mind, because controller is the only person responsible on lawful processing of the data.[51] For example, in these circumstances, controller has no instrument to change offered contractual provisions, even if they are against the data protection directive. The last issue will not avoid controller's responsibility to process data lawfully according to the directive rules[52]. In the end we may receive picture, when user/controller has no power to alter standard rules of offered contract, even if the principle of lawful processing is violated. Regarding the said reason it remains relevant to consider user as a data subject, as controller's responsibility will be under question if user will be considered as a controller.

---

[47] "Directive 95/46/EC," 6 (1) a.

[48] Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 7., Hon, Millard, and Walden, "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now," 103., "Article 29 Data Protection Working Party, WP 196," 7. "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe,'" 10. Gutwirth, *Computers, Privacy and Data Protection an Element of Choice*, 386.

[49] Mantelero, "Cloud Computing, Trans-Border Data Flows and the European Directive 95/46/EC: Applicable Law and Task Distribution," 3.

[50] "Article 29 Data Protection Working Party, WP 196," 8. Hon, Millard, and Walden, "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now," 84.

[51] "Directive 95/46/EC," article 6 (1) a, 6 (2).

[52] Ibid., article 23.

Secondly, at the same time we should point out that users are customers of the electronic contract as well, they are subject of data protection. How they can fulfill obligation of controller and at the same time be subject of the protection? In general, if we pose obligation from one side, the same party could not be protector as well. Controller protects data user's rights. This could be the question in practice. So provision data controller as a user should have ambiguity in electronic contracts.

Counterargument considering user, as a controller has the European data protection supervisor ("EDPS").[53] Supervisor asserts that the service provider could be a controller, because controller should comply the requirements according to the directive, such as insure data security and process data only for the legitimate purpose.[54] It is controller's responsibility to take technical and organizational measures for the processing.[55] At the same time, user/controller has no technical resource to control data and take any security measure for data protection.[56] However, EDPS recommends that user could be a joint controller of the data together with service provider. Usually, cloud service provider has the technical equipment and infrastructure to process data[57], not the user.

Especially, when we deal with the case of service provider using SaaS infrastructure user could have the problem of taking reasonable security measures, because the latter has no direct control over the infrastructure.[58] At the same time one should take into account that controller is responsible for data accountability.[59] Namely, the controller is duty-bound to

[53] Later in the text used as EDPS is watching that all EU institutions and bodies respect the rights of citizens while processing data. For further information you can visit http://europa.eu/about-eu/institutions-bodies/edps/

[54] Peter, Hustinx, "Panel IV: Privacy and Cloud Computing 'Data Protection and Cloud Computing under EU Law.'" Gutwirth, *Computers, Privacy and Data Protection an Element of Choice*, 386; 389–390. Hon and Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4," 24.

[55] Ibid

[56] Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 7–14.

[57] "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe,'" 12.

[58] Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 29–30.

[59] "Directive 95/46/EC," article 10.

"carry out audit, adopt internal policy and process to implement requirements by data protection directive."[60] Clearly, the user is not in a position to fulfill these obligations. Furthermore, considering user as a data controller can cause problem with respect to the applicable law. If user/controller has a non-EU establishment, the jurisdictional problems may arise[61] and EU law may not be considered applicable in such cases. This will be further discussed in details in Chapter 3 of this study. For the purposes of the foregoing discussion, it is safe to conclude that the arguments against the user being a controller does exist and it is considered more appropriate measure to consider user as a data subject only.

Significant criterion defining controller is the "means of processing." The term "means"[62] refers to technical and organizational facilities for implementation of the data processing.[63] But it does not necessarily imply using only technical means of processing of information but rather includes the way how the processing can be done, which data should be processed, deleted etc.[64]

"Means of processing" could be a program, where processing could take place and controller should be equipped by such a "means of processing" in order to process data.[65] This is crucial problem for the user/controller in electronic contracts given that this party does not have any technical resources to process data. User can be an originator of the data message, write online their name, address, bank account number and other requisites necessary to enter into online electronic contract. For example, in case of online booking services, user gives order to process data in EU territory or outside EU. But the problem here could be that user has no possession of the equipment. Therefore, it is highly advised to regard the service provider as a controller. Usually service providers are equipped with and possess software program, so

[60] Wong, "Data Protection," 56.
[61] Gutwirth, *Computers, Privacy and Data Protection an Element of Choice*, 390.
[62] "Article 29 Data Protection Working Party, WP 179," 8; 20. "Article 29 Data Protection Working Party, WP 56," 8. The English wording mean for the purposes of the directive is used as an equipment, because it is considered that this is the proper word could be user in these cases.
[63] "Article 29 Data Protection Working Party, WP 169," 14, 4.
[64] Ibid., 14. Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 6–7.
[65] "Article 29 Data Protection Working Party, WP 169," 14.

called equipment to process data. Thus, it is more reasonable to consider the user as data subject and leave the controller's functions to the service provider.

Nevertheless, users have the possibility to use service provider's infrastructure and be a controller of the data. In case of SaaS service, user may use the program of the service provider and is considered as the controller of the equipment as well.[66] Using other party's infrastructure could be considered as owning equipment for the purposes of the definition of the controller. Precisely, law should be interpreted less strictly in this respect so that the user/controller is not required to possess any "means", "equipment" of its own and can use those owned or operated by the service provider.[67] At the same time it is not obligatory for the user to have physical possession of the equipment as long as it can avail itself of the possibility to use service provider's program/equipment for processing data. However, yet another issue can be raised in this respect. Namely, service provider can save user's data on the hardware.[68] This could cause the problem of data protection, since when the data is stored on certain medium, the controller is not the only party able to control the data and hence responsible for its security. This is because the third party, such as service provider, has access to such data and can back it up or otherwise store the data on the server, without any due permission of the controller. However, user has no ability to control data location, i.e. user may not track down the particular server where the date is stored. And again, this brings up the issue of identifying the proper applicable law. This issue will be analyzed in details in Chapter 3 of this thesis when discussing the applicable law.

The future of the controller's responsibility depends on the commission regulation. The issue on defining user's role as a data controller becomes more complicated in data protection regulation.[69] As a starting point, the Regulation attempts to be more precise on the functions of controller. According to the Regulation, controller not only defines the purpose of the

[66] Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 9–13.
[67] Ibid., 9–13; 11. Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 18–19.
[68] Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 9–13.3
[69] "Commission Proposal COM(2012) 11 Final 2012/0011 (COD) C7-0025/12.".

processing, but also the conditions thereof as well as the means of processing. The Regulation introduces the term "conditions" while the meaning of the term "means", as defined above, remains unaltered. This does not bring any dramatic change to the definition of controller and the term "conditions" can be understood as the rules on how data should be processed and in which circumstances.

The role and the responsibility[70] of the controller is strengthened in the Regulation and for the purposes of this study it is important to determine how it could influence the definition of user as a controller in cloud computing service. Article 29 data protection working party considers that broader role and function of the controller will help for the protection of privacy issues, especially national data protection authorities can better execute mandatory provisions of law.[71]

According to Article 5 (f) of the Regulation, data should be processed under the "responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation." This article suggests that apart from increased responsibility, the administrative burden of proof of fair processing and compliance with the law has been shifted to the controller.[72] Moreover, Article 22 of the Regulation increases the responsibility of the controller and it is highly doubtfull that the user in the cloud computing service is expected to fulfill requirements in these circumstances, when user has no actual knowledge of the proposed rules.

The additional formal requirements introduced by the Regulation likewise increase the liability of the controller. Namely, controller is now obliged to represent documents and fill them according to Article 28 of the Regulation in order to prove that processing was carried out in full compliance with the applicable law. In case of legal entities and other institutions,

[70] When I will mention the responsibility of the controller, in my thesis reader should take into mind that I will not discuss all kind of responsibility of the controller, because it is not the main focus of my thesis. I will mention the responsibility which is connected to the contractual obligation between controller and processor, article 17 Directive and article 26 of Regulation.
[71] "Article 29 Data Protection Working Party, WP 168," 3.
[72] Digital Single Market Group, "Position Paper on the Proposed General Regulation on Data Protection," 11.

which are vested with the controlling power, this formal side of the controller functions is likely to be easily dealt with. Namely, such legal bodies usually have lawyers and consultants who can provide legal advice and handle the paperwork. However, what about individuals/users? Who will monitor their actions and their compliance with imposed obligations, especially in cloud computing cases? Therefore, there is a reasonable fear that Article 22 might not work in practice since the controller does not itself process the data and has less ability to control the actions of the actual processor.[73] This is all the more true with respect to the condition processor controller relationship. Processor should execute the obligation of processing, entrusted party or wholly to him by the controller.[74]

To sum up proposed issues, it should be highlighted that in most sources, users are considered as a controller in cloud computing scenario. I have showed the positive and negative effects on the said statement. The fact is that data protection issue is mostly depended on function of controller of the data, such as lawful processing of personal data. That's why it was recommended to consider user as data subject for enjoying with the privileges of the customer in electronic contracts. However, we could not ignore that users are the main figures in electronic contracts. They are the initiator of the processing, handle the processing operation: in which direction should be sent data, they give the request to book hotel online for example. They control the data processing operation. In the end we should be careful defining function of the user, as a controller. Several circumstances should be taken into consideration and case by case study will show if the user is the controller.

[73] Ibid., 11–12.
[74] "Article 29 Data Protection Working Party, WP 168," 19.

2.2.2 The Function of the Service Provider in Electronic Contract

The Data protection directive, Article 2 (e), defines the processor an individual or legal body, which processes data on behalf of the controller. The limited scope of processor's activity, receive directions from the controller, does not necessarily mean that processor should not be an independent body.[75] In cloud computing services, user gives directions to the website to process data and gives order to book hotel within or outside the EU territory. Even though, service provider is independent body, for the purposes of the hotel-booking example discussed here and mostly the EU established company.[76]

The service providers are considered to be data processors in cloud computing service.[77] In this respect, one has to recall the landmark case of *Google v. Italy*, were the European Court of Justice considered service providers as data processors, whereas the cloud computing users were qualified as the controllers.[78]

The relationship between service provider and user is regulated by legally binding contract, defining the duties and rights of the parties.[79] Whether the same body could be considered as controller and processor in the contract is subject to controversy. In general, contract is a bilateral agreement and one party may not be in a legally binding position from the both sides, this may create obstacles in the controller-processor relationship. One of the important cases, which deal with contractual relationship between controller and processor, is a so-called SWIFT case.

---

[75] "Article 29 Data Protection Working Party, WP 169," 25.
[76] for example booking.com hostelworld.com
[77] Hon and Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4," 4. Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," 7., Hon, Millard, and Walden, "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now," 103., "Article 29 Data Protection Working Party, WP 196," 7. "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe,'" 10.
[78] Sartor and Viola de Azevedo Cunha, "The Italian Google-Case," 1–2.
[79] "Directive 95/46/EC," article 17.

Worldwide Interbank Financial Telecommunication (SWIFT) with Belgium established institution transferred personal data to the Office of Foreign Assets Control (OFAC) of the United States Department of the Treasury (UST). The Belgium data protection commission came into conclusion that SWIFT's US branch violated privacy with regard to processing data from the EU branch to the United States.[80] The data furnished to the US branch concerned the EU citizens' bank transfers between financial institutions, regardless weather messages were processed within EU or in the third countries.[81]

Interesting point is that according to the contract between parties, SWIFT was considered as a controller. SWIFT decided means and purpose of the data processing. The management office of the SWIFT decided the level of data, which should have been processed.[82] The working party considered that SWIFT fulfilled function of data processor, while transferred data to the financial institutions.[83]

The opinion of working party showed that regardless of contractual provisions, financial institutions were data controllers as well.[84] They were taking part to determine means and the purpose of the processing, had direct contact with the individuals and played an important role "in the execution of the international payment orders of their clients."[85] However, as in the SWIFT case, financial institutions received directions to process data.[86]

To sum up, SWIFT case casts some light over the controversy. Firstly, in SWIFT case two contractual counterparts – SWIFT and financial institutions - shared processor and controller responsibilities. According to the case, when one party is a controller, the other party must be a processor and vice versa. Therefore, the function of a processor may not be combined with that of the controller in one and the same party to the contract. Secondly, contractual

[80] Belgium commission's decision is available here: http://www.privacycommission.be/
[81] "Article 29 Data Protection Working Party, WP 128," 7–8.
[82] Moerel, "Back to Basics," 107.
[83] "Article 29 Data Protection Working Party, WP 128," 11. "Article 29 Data Protection Working Party, WP 169," 9.
[84] "Article 29 Data Protection Working Party, WP 128," 13.
[85] Ibid.
[86] Ibid.

agreement between parties and definition of the controller and the processor in the contract is not decisive.[87] SWIFT case showed that several circumstances are to be taken into account to fulfill requirement of the law – define controller and processor in each case. This can create obstacles in practice. On the one hand, there must be a legally binding contract between processor and controller for the processing operation of the data. However, on the other hand, the same contractual agreement turns out not to be decisive and in each case the fact-based assessment must be carried out as to who controls the data and who processes it.

Another important point worth discussing is the contractual arrangements between the controller and the processor. According to the data protection directive, Article 17, data processor has the obligation of data security and according to Article 16 of the data protection directive the same party has confidentiality obligations. These duties are defined by the contract between the parties, where controller delegates his obligations to the processor to fulfill lawful processing of the data.[88] As a result of such contractual rearrangements, it is the processor who is left with the most of the duties with respect to data protection. This however, does not mean that the controller will be free from its share of responsibility.[89]

The Data Protection Regulation specifically deals with the controller-processor relationship. Article 30 defines that obligation on data security is on controller and processor. Although, liability for data breach still remains with the controller, as in case of data protection directive, Article 23. The dues and obligations of the data controller under the new regulation have already been discussed in details above in this thesis. Therefore, here it is enough to mention that Article 26 is more detailed about the contractual obligations between the controller and the processor. Nevertheless, overall framework of the regulation concerning controller-processor relationship has not been changed.

---

[87] "Article 29 Data Protection Working Party, WP 169," 8–9. Hon, Millard, and Walden, "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now," 103. Moerel, "Back to Basics," 106–109.
[88] "Directive 95/46/EC," article 17.
[89] Ibid., article 23. data protection directive, where controller has the responsibility on the violation of the processing operation. "Commission Proposal COM(2012) 11 Final 2012/0011 (COD) C7-0025/12," article 31.

In light of the above, a question remains as to whether it is at all necessary to have liabilities contractually agreed between the controller and the processor, if the controller will be responsible on every decision of unlawful processing? The answer is probably positive, it is important that controller and processor have a contract and processor is aware of the obligations related to the processing. At the same time, controller should be careful and follow the processing operations as well. Because the principal party responsible for the lawful processing of the data is the controller. Notably, the decision in SWIFT case brought some confusion in this respect when holding that contractually agreed division of spheres of responsibility of the parties does not mean that the party is completely exempted from liabilities falling within the scope of the responsibilities of the other party. Such as if we define processor in the contract, it may appear that another party should share responsibility and be obliged to process data. The significant factor is an opaque nature of the provisions of the Directive. The possibility to decide the functions and the role of the responsible persons – controller and processor, on case-by-case basis, leaves the broad discretion to the court. This flexibility and room for interpretation undermines predictability and legal certainty. Precisely, directive may be interpreted as broad as to cover not only EU established controllers but also non-EU established ones and widen the vast of profound field. Yet the provisions on duties of the processor and the controller are vague. One may even consider this to be an intentional decision of the drafters to give flexibility to the legal authorities to extend the application of EU directive provisions worldwide, broaden EU law applicability boundaries and jurisdictional provisions of the data protection directive.

2.3 The Concept of Information Uploaded in Electronic Contract

2.3.1 Definition of Personal Data

To analyze the definition of personal data and give the answer if data uploaded on the website in time of e-contracts is personal data first of all we should analyze definition of personal data. Important point is that all the information does not fall under the definition of personal data. Information[90] should be related to the person and give grounds to identify that person. This kind of definition should stay for a while, because whatever law could be changed the main purpose of personal data definition is to identify the said person[91]. To identify person means that he/she should be distinguished from others [92] directly or indirectly.[93]

Interesting point could be how natural person can be identified? The answer is by 'certain identification number or other factors', such as **'**physical, physiological, mental, economic, cultural or social identity'.[94] These factors are general and directive text needs further specification. For discovering personal data concept several aspects should be taken into account, such as telephone number or car registration number, or social security number, or passport number which are combination of criteria for identifying person. Data protection regulation is accurate on this issue and by the development of new technologies broadens the scope of personal data identification: such as defines that one factor to find out personal data is 'location data and unique identifier'[95].

The Data Protection Regulation is close to the 1995 directive recital 26, which gives the same meaning of the data identification. For the identification data 'all the means likely reasonably'

[90] lee bygrave, p 42 Bygrave, *Data Protection Law*, 42.
[91] Ibid.
[92] "Article 29 Data Protection Working Party, WP 136," 12.
[93] For the detailed interpretation see Article 29 data protection working group opinion on concept of personal data 4/2007, WP 136
[94] "Directive 95/46/EC," article 2 (a).
[95] "Commission Proposal COM(2012) 11 Final 2012/0011 (COD) C7-0025/12," article 4 (2).

should be used. The wording **'likely'** should mean 'probability of identification' and such as **'reasonably'** should be considered as a 'difficulty of identification'.[96]

Interesting point is that how new regulation deals with data identification issues, if exists obscurities on personal data definition. New regulation text[97] becomes unclear when defines that not only controller could identify the data subject, but any other person as well. What does it mean? In some situation processor may have function of identification person, because contract between parties give right to the processor act on behalf of controller and deal with data subject identification. Though, in case of new regulation it becomes vague who could be any other person, manage with personal data criteria. Directive approach gives the possibility to go further than data protection provisions, who can be an identifier of the data.[98] As we mentioned to the previous chapter, only the controller can share the responsibility on lawful processing of data, so it is under question according to the law any other party, rather than controller can take responsibilities implied in data protection directive.

Another important issue about personal data is 'all circumstances' which should be taken into consideration to identify the person. Data Protection Regulation is criticized for such kind of provisions, because not all kind of information can identify the person.[99] Such as controller may collect data, which is pseudonym data For example, it should be clear that if the person is not identified directly that person should not fall under scope of the Data Protection Regulation.[100] EDPS supervisor is against also covering pseudonym data in new directive and consider that in these conditions it will be hard for the controller to fulfill the principles of lawful processing.[101] But at the same time, according to the new regulation, article 10 (2), if controller can't identify person, he\she is free from the responsibility. This provision broadens the doubt that new regulation has serious problem on data interpretation, together with

[96] Bygrave, *Data Protection Law*, 44.
[97] "Commission Proposal COM(2012) 11 Final 2012/0011 (COD) C7-0025/12," article 4 (2).
[98] Digital Single Market Group, "Position Paper on the Proposed General Regulation on Data Protection," 7.
[99] Ibid., 8.
[100] "Commission Proposal COM(2012) 11 Final 2012/0011 (COD) C7-0025/12."Article 10 defines that controller is free of the obligation gathering pseudonymous data. 8 Digital Single Market Group, "Position Paper on the Proposed General Regulation on Data Protection," 8.
[101] "Additional EDPS Comments on the Data Protection Reform Package," 3.

provision that any person could be a data processor and new regulation now rescues the responsibility to the controller in time of pseudonym data.

2.3.2 Information Uploaded on the Website – Personal Data?

In the previous chapters we defined the relationship between controller and processor, the role of the user in electronic contract and service provider. Now it is important to discuss if the data which user uploads to the cloud computing service are considered as personal data. In the cloud computing service websites, I am focusing to, users are required to upload: name, nationality, gender, address, telephone number, email address, credit card details.[102]

The information we upload on the website I consider that is personal information, because gives ability to service provider identify the user. However, European Court of Justice defined that "referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data [...] within the meaning of [...] Directive 95/46/CE"[103] The same way, in the other decision as well was defined that name and address of the person is identification tool and is considered as personal data[104].

[102] http://www.booking.com/content/privacy.en-gb.html?dcid=1&lang=en gb&sid=6a7db4f846f81f18fe5bb1044ba75b9e
http://www.hostelworld.com/securityprivacy.php
[103] Criminal proceedings against Bodil Lindqvist, para 27 (European Court of Justice 2003), para 27.
[104] College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, para 42–43 (European Court of Justice 2009), para 42–43.

However, financial information, such as bank statements is considered as a personal data according to the UK court, which gives the definition according to the EU directive as well.[105] Moreover, in case of SWIFT[106] financial information processed about the clients were considered as a personal data. The above mentioned statements give me possibility to conclude that according to the data protection directive, name, address, financial information is related to the identification issues to the users and will fall under the definition of personal data. In conclusion we can say that service provider receiving information from the user, while booking hotel is considered as a personal data.

[105]Chalton, "The Court of Appeal's Interpretation of 'Personal Data' in Durant v. FSA - a Welcome Clarification, or a Cat amongst the Data Protection Pigeons?," 177.
[106] "Article 29 Data Protection Working Party, WP 128," 5.

3 Applicable Law Processing Data in Electronic Contracts

This chapter will decide applicable law criteria, as it is the most important focus of my thesis. Before answering question how EU law apply in case of electronic contract, in the first part I will evaluate if jurisdiction and applicable law are the same for the purpose of EU directive.

In the second part I want to define in general directive provisions if they cover European established company, what is the establishment criteria and how it effects on deciding applicable law? Does it have main power or other criteria prevail, such as processing data in the context of activities. Another issue is if company has non-EU establishment does data protection law apply? What is the main factor applying European law at this case?

In the third part I will analyze the influential factors in defining choice of law and try to answer question is law broad enough in reality or in practice may occur disagreements between law and court decisions.

3.1 Applicable Law Concept – Different from Jurisdiction?

One of the crucial and important points while dealing with applicable law is differentiating the concept of "applicable law" from the concept of "jurisdiction" for the purposes of EU directive. The point of interest is weather these notions are identical, merging in one broad issue such as globalized jurisdiction. Article 29 data protection working party is not clear enough on this issue and draws distinction between jurisdiction and applicable law. However, Article 28.6 of the data protection directive unifies jurisdiction issues with applicable law and

grants the right to national authorities to decide the case in accordance to their jurisdiction.[107] Several sources may serve as an example for arguing that jurisdiction and applicable law is the same concept for the purposes of data protection directive. Svantesson,[108] although agrees to the assumption that applicable law and jurisdiction are different concepts, states that when dealing with data protection issues the former serves the same purpose as the latter. According to Kuner,[109] article 4 of EU directive contains issues on choice of law and jurisdiction as well. He suggests that choice of forum is identical with choice of law matter for the purposes of EU directive when there is dispute between service provider and the customer.

Practice demonstrates that article 4 defines jurisdictional rules for the controllers.[110] It is important to outline, that jurisdictional rules usually point to more than one forum, while applicable law states only one.[111] In internet it is difficult to identify one forum, for this reason in some circumstances applicable law articles are equalized with jurisdiction.

It is difficult to draw uniform approach from the legal literature with regard to the issue of distinction between jurisdiction and applicable law. However, it can be stated that no distinction is made between these 2 concepts in the EU Directive itself. The provisions of the directive are too broad and are not dealing with this matter precisely, these provisions even overlap jurisdictional issues. Namely, article 4 of the Directive dealing with applicable law identifies precondition for applying EU law. By virtue of the said article, non-EU established company can also be subjected to EU data protection law. Thus, as it was demonstrated above applicability of EU law is extended from EU territory and can affect non-EU established company. Consequently, EU authorities will have jurisdiction to decide the case involving such non EU-established company.[112] Another example would be processing data in the context of activities. As it was already discussed above, controller, who processed data in the

107"Article 29 Data Protection Working Party, WP 179," 10.
108 Svantesson, *Private International Law and the Internet*, 11.
109Kuner, "Submission to the 'Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union'," 3–4. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law Past, Present and Future*, 25.
110Kuner, *European Data Protection Law*, 112.
111Svantesson, *Private International Law and the Internet*, 12.
112"Directive 95/46/EC," article 4 (1) c..

EU context might have non EU establishment, engaged in processing data without using EU equipment. In this case EU authorities might still be authorized to decide the matter, but only if the activities were carried out in the context of EU establishment. In these circumstances, both with regard to non-EU established company and non-EU establishment parent company, applicable law would decide the jurisdictional matter over the company if the data was processed in EU territory by these companies. Especially if we take into account the existence of article 28.6 data protection directive, when authorities of the member state are competent to decide the case[113]. However, in data protection Regulation the wording 'applicable law' is replaced with the wording 'territorial scope'.[114] The reason for that could be that for the purposes of data protection applicable law is considered to be identical with jurisdiction.

Extension of the EU jurisdiction and treating applicable law as a similar concept with jurisdiction, does not exclude application of the non-EU law in certain cases. For instance non-EU law could be applicable in case of data transfer to the third country, such as directive tries to define jurisdiction and requiring adequate level of protection concerning article 25 and 26 of EU directive.

And lastly, it shall be stated that in order to avoid jurisdictional problems following should be taken into consideration: general harmonization of directive, cooperation between regulatory authorities, cooperation on jurisdiction between data protection world is necessary to solve jurisdictional difficulties.[115] Although the above stated suggestion might be effective, SWIFT case[116] demonstrated that certain issues may arise in practice, which in contract should not be taken into consideration. At the same time, it shall be noted that law or contract alone is not sufficient enough for dealing with every practical aspect that may arise; for this reason

113 The same idea is written to Kuner, "Data Protection Law and International Jurisdiction on the Internet(Part 1)."
114 Article 3 "Commission Proposal COM(2012) 11 Final 2012/0011 (COD) C7-0025/12," article 3.
115 Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)," 242–244.
116 "Article 29 Data Protection Working Party, WP 128."

cooperation between parties might be required, for instance to negotiate safe harbor principle, for the transborder flow of data between US and EU.[117]

3.2 Major Factors Defining Applicable Law in EU Established Company - General Overview

3.2.1 Establishment Place of the Controller

The key factor to determine applicable law is the establishment place of the controller, according to the directive[118] article 4 (1) a. At the same time the establishment place is considered 'country of origin' of controller.[119] While deciding establishment place of company several conditions may be raised at the same time. For example, establishment of controller may occur to the third country, but still may be used European state's law[120]. However, controller may have the establishment in different member state, but the determinative factor here should be the other criteria, such as the context of the activities, when the processing was fulfilled.[121] Regarding this statement, firstly we check if the controller has establishment to the EU territory, if the answer is positive, then we check if the activities were in the context of EU establishment.[122] However, the establishment of the controller may not be decisive, if we do not have the second criteria, activities performed in the context of processing data[123]. The above mentioned statements are too general and are the issue which may be raised in deciding applicable law in EU established companies. I will try to analyze and explain provisions of the article 4 (1) a step by step.

117"2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce (notified under Document Number C(2000) 2441) (Text with EEA Relevance.)."

118 "Directive 95/46/EC,"

119 Moerel, "Back to Basics," 93.

120 "Directive 95/46/EC," 4 (1) c.

121 "Article 29 Data Protection Working Party, WP 196," 7.

122 Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 8.

123 Moerel, "The Long Arm of EU Data Protection Law," 3. In the article it is mentioned commentary of Damman and Simitis (n 10), at 127–8

The first criteria is controller's definition, which is discussed in the second chapter. The next decisive factor is meaning of establishment, which is defined by the text of recital 19:

establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements (and that) the legal form of (..) an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect.

The meaning of establishment may cover many type of business activities, such as parent company, branch or subsidiary processing data may be considered as an establishment of the company. We should be accurate while regard as the branch or subsidiary establishment, because many activities in electronic commerce is not constituted as an establishment[124]. Mainly, there exists assertion that parent company has access on software system and other system where processing takes place and that's why it may be a controller of the data. For the same reasons company's branch may have access to the data as well.[125] For example company can easily control the data of the employees and process them for the reasons of the directive. However, according to the decision of European Court of Justice, branch can be considered establishment place, if the office activities has a permanent nature and has the ability to negotiate to the third parties independently.[126] Though, defining branch, subsidiary or parent company under the meaning of article 4.1.a or c depends on the several criteria, not only establishment place of the controller, also context of the activities in which the processing took place, using equipment with non eu-established companies as well.[127]

European court of justice interpreted company's establishment place, which covers "both human and technical resources".[128] ECJ decided that technical equipment such as

[124] Kuner, *European Data Protection Law*, 83.
[125] Moerel, "Back to Basics," 99.
[126] Blanckaert & Willems PVBA v Luise Trost., Summary, para 6 (ECJ 1981), Summary, para 6. Somafer SA v Saar-Ferngas AG, Summary para 2; 12 (European Court of Justice 1978), Summary para 2; 12.
[127] Moerel, "Back to Basics," 103.
[128] Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt, para 14 (European Court of Justice 1985), para 14.

"company's server, which is not situated in a country of a service provider could be considered a stable arrangement for the meaning of the establishment.[129] Although, "judge refused to consider computer means as a virtual establishment[130]." The same idea is written in article 29 data protection working group opinion 56 and explained that in case of a server or a computer, it is not considered as an establishment, as it is simply a technical facility or instrument for the processing of information.[131] However, court mostly pays attention on economic activity of the company for an identified period while deciding establishment place of the company.[132]

Although, at the same time court interpreted that: *"An establishment of a company in a member State other than its main place of business cannot be deemed to be the place where it supplies its services ... unless that establishment has a sufficient degree of permanence and a structure adequate, in terms of human and technical resources, to supply the services in question on an independent basis".*[133] This decision is more precise and defines that all criteria should be taken into account, not only technical resources or quality of business activities for the establishment place.

Interesting issues arises as well if the third party acting on behalf of the controller could be considered as an establishment place of the controller. This issue is more complicated if we talk about non-EU established companies.[134] ECJ considered that if agent's legal status give the permission freely represent the company, without any further influence of the parent company in time of negotiation will not be considered as the agent.[135] In conclusion we can say that ECJ does not give exhaustive list of activities which should be considered as an company's establishment place, the criteria is depended on case by case study.

[129] Ibid
[130] Ibid
[131] "Article 29 Data Protection Working Party, WP 56," 8. Hon and Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4," 9.
[132] The Queen v Secretary of State for Transport, para 20 (European Court of Justice 1991), para 20.
[133] ARO Lease BV v Inspecteur van de Belastingdienst Grote Ondernemingen te Amsterdam, summary para 15–16 (European Court of Justice 1997), summary para 15–16.
[134] Moerel, "The Long Arm of EU Data Protection Law," 8.
[135] Blanckaert & Willems PVBA v Luise Trost, summary para 13 (European Court of Justice 1981), summary para 13.

3.2.2 Context of the Activities Performed by the Controller

The establishment criteria will not have effect in deciding applicable law if we do not have the second and the most important condition, process data in the **'context of the activity'** of the controller**.** This means that activities, fulfilled by the data controller's establishment place should be in the context of processing data.[136] Also controller's activities should have a purpose to process data in EU territory. As we can see, establishment of the controller is not enough for defining applicable law. There should be always close connection between processing data and the establishment place of the controller.[137] Mostly, controller's activities on processing data should be determinative factor, that's why, controller without EU establishment may fall under the definition of EU establishment as well if the activities were in the context of EU establishment.[138]

Also we should also bare in mind that the nature and the place of the context where processing carried out is determinative factor as well. This means that the customer's data maybe processed in the context of the activities outside of the EU applicability but EU law still will be applied.[139] Moreover, when deciding applicable law there should exist question - who is doing what? The main attention also on this case takes the nature and degree of the activities.[140] We also should take into consideration that these issues are too theoretical and the practical point of view will be significant at these cases.

---

[136] Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 9. "Article 29 Data Protection Working Party, WP 196," 7.
[137] Kuner, *European Data Protection Law*, 117.
[138] "Article 29 Data Protection Working Party, WP 179," 9. Mantelero, "Cloud Computing, Trans-Border Data Flows and the European Directive 95/46/EC: Applicable Law and Task Distribution."
[139] "Article 29 Data Protection Working Party, WP 179," 9.Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 9.
[140] "Article 29 Data Protection Working Party, WP 179," 14.

Another theoretical issue it controller's establishment place in several states. This does not mean that controller may avoid the responsibility, it should be guaranteed that each of the establishment applies to the same level of the data protection. At this case more than one member state's data law should be applicable. This provision may create problems in the future on deciding applicable law, because not in every case of joint controlling could create jointly applicable law, one law should apply. At this situation the significant factor could be the activities where processing was fulfilled, which member state's law had a close connection to the activities and the processing. This affirmation may take place also when there is the processing in the branch office' activities, main factor as we mentioned is the context of the activities where processing took place. However, it should be used technical equipment not virtual establishment, for example computer or server could not be considered as an establishment as I mentioned before, in 3.2.1. subchapter.

3.2.3 Processing Data via Equipment

Analyses of the service providers in cyberspace showed that European citizen's data could be processed in case of non-EU established companies.[141] The authors of the directive defined that in case of non-EU established companies, directive could be enforced if the service provider using the equipment[142] situated in EU territory. Directive article 4 (1) c considers EU law applicable regardless the fact that controller has no establishment in EU but processes data in EU using equipment situated in EU territory. The provision of directive shows that the legislators found out the way for non-European companies and service providers to be under the influence of directive and the concept of "using EU-equipment" was equalized to the criteria establishment for the purposes of applicable law.

[141] "Directive 95/46/EC," article 4 (1) c.

[142] The working party considers that the word "equipment" and "means" used in EU directive article 4 (1) a and c and the "means" used in controller definition has the same meaning regardless the fact of difference meaning in english language. "Article 29 Data Protection Working Party, WP 179," 20.

The main factor on using equipment could be the purpose to process data, because not every case sets under the meaning of article 4.1.c. Though, mostly in every case, the purpose for non-EU established service provider could be transferring data from EU. This means that from the one hand almost every company using equipment which is established in EU territory would be under the scope of this article for the purpose of directive to process data.[143] Although, this is the easy way to decide the issue on applicable law, because first of all there are criteria and service provider should comply them. The main question is what do we mean under the equipment?

The interpretation of equipment includes human and/or technical intermediaries, such as "in surveys or inquiries. As a consequence, it applies to the collection of information using questionnaires, which is the case, for instance, in some pharmaceutical trials".[144] However, equipment is not necessarily "solid, tangible or materially substantive".[145] The directive wording on equipment is vague. The issue becomes more complicated when it is not defined if controller needs to have the whole ownership or control over the equipment. According to the working party opinion it not decisive, controller owns or controls it.[146] That is the reason for the Kuner[147] to define that English word equipment is not appropriate here, because it should be possible that controller did not have full control over the equipment.

However, counterargument could be that determinative factor defining equipment could be the degree of control, the controller's power to determine the way how equipment should work, make proper decisions on the procedures and substance of the data by using equipment to process data. However, controller by using equipment should have the possibility to define which data should be collected, stored, transferred, altered, deleted etc.[148]

[143] Ibid.
[144] Ibid.
[145] Bygrave, "Determining Applicable Law pursuant to European Data Protection Legislation," 255.
[146] "Article 29 Data Protection Working Party, WP 179," 20.
[147] Kuner, *European Data Protection Law*, 118.
[148] "Article 29 Data Protection Working Party, WP 56," 9.

According to the directive, exclusion could be case when equipment is used for the means of transit data regardless the fact that it is situated in the EU territory. The main idea of the article as I mentioned is that the processing should have the purpose by using the equipment. However, in practice it is really hard to differ if the controller using equipment on the purposes of processing data or just for the transiting data. Mostly, in every case using equipment, established in EU territory should be a reason to consider it processing data, especially when we are talking about EU citizen's data. However, in cloud computing cases we considered that it is not obligatory that the user had ownership on equipment, may user service provider's equipment and still will be the controller of the data.

Practical experiences is important to define the "use of equipment", such as personal data collected from the user's computer in case of cookies, Javascript banners should fall under the meaning of equipment[149]. Interesting situation occurs, when the service provider has no EU establishment and processes the data of the EU citizens. Here should be two cases: using cookies and using data centers outside EU. I will discuss them to the next chapter.

3.3 Problematic aspects of defining applicable law in electronic contracts

3.3.1 Practical Examples of Processing - Easy to Choose Law?

In the beginning of second chapter I described briefly that in electronic contracts service providers are cloud computing service providers. Formally, similar requirements apply in specifying applicable law for cloud computing service as it was discussed in the former chapter. Firstly, we should decide if establishment place of controller was EU, then activities in the context of the EU establishment, if the answer is positive in both case, we use EU

[149] "Article 29 Data Protection Working Party, WP 179," 21.

law.[150] But in reality, may be formed ambiguity between general criteria of applicable law and cloud computing, problems may arise in deciding applicable law. Mostly this chapter and the next one answers thesis second question if the law is too broad and if applicable law requirements are theoretical?

For analyzing abovementioned statement I would like to give examples from the websites, I am focusing on my research and I will discuss applicable law issues where processing took place in the context of the EU activities. In these circumstances I will separate three issues: firstly, websites defined EU law could be applicable. Is this rule mandatory or other conditions should be taken into consideration as well? Second issue will evaluate how applicable law criteria work in practice. And lastly, paper will assess the future perspective of choice of law regulations based on the EU directive and Regulation. Does law provision broadens the applicable law in worldwide or law is too theoretical.

Starting with the first issue, terms and conditions of the websites designate applicable law to be the EU law.[151] However, this does not entail that EU law will apply in each and every case. Especially I pointed out that contract between parties in cloud computing does not necessarily mean that law binding regulation does not apply.[152]

The European commission clearly interpreted that *"while the applicable laws can be defined, to a certain extent in the respective services agreement with the provider, there can also be mandatory laws which cannot be derogated by contractual agreement…"; "Especially when providing services to customers in multiple jurisdictions, it is a significant burden to understand and comply with all laws and regulations."*[153]

[150] Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 8–9.
[151] http://www.booking.com/general.en-gb.html?dcid=1&lang=en gb&sid=ecabfd4cd95f5afa3f2080bd637e9437&tmpl=docs%2Fterms-and-conditions; http://www.hostelworld.com/hosteltermsandconditions.php
[152] Bradshaw, Millard, and Walden, "Contracts for Clouds," 195–196.
[153] EUROPEAN COMMISSION, *Cloud Computing: Public Consultation Report*, 2.

The above statement is based on the Rome I regulation, article 6 (1) [154] where consumer's place of establishment is decisive.[155] Furthermore, article 6 (2) states that in case parties agreed on the choice of law in the contract, they still shall take into consideration the law which would be applicable in case of no agreement between the parties. Similar provision on applicable law can be found in Brussels I regulation, article 15 (1), which interprets jurisdiction according to the consumer's domicile, when there is a contract between consumer and the business regarding sale of goods, or other type of commercial activities.[156] Analyzes of the law demonstrated that parties contractual agreement is not decisive in every case as data protection legislation shall also be taken into consideration. However, when it comes to electronic contracts where the user is at the same time a consumer, relevant provisions on consumer protection will also have influence on contractual provisions regarding the choice of law. Thus, data protection law has decisive influence on electronic contracts. Furthermore, examples from the website shall be provided for further evaluation of the question at hand. Point of relevance would be the question of applicable law when activities are performed on EU territory.

The question about the applicable law is clear if EU established user\controller uploads data and books hotel in the EU country. In this case EU law will be applied. Another example would be when a controller/user with non-EU establishment processes data on the EU territory for ordering hotel in the EU country, which law could be applied? The important factor with the non-EU established user would be if the activity in question – ordering hotel in EU territory - was carried out in the context of EU establishment. It has to be taken into account that user asked the service provider to book hotel on EU territory, as well as the fact that service provider has EU establishment. This means that EU service provider is processing operation and is the regulator of the content as well within in EU establishment. It does not affect service provider's role, as a data controller. User he/she delegated the right to the service provider to process data and performed activity in the EU territory, book hotel for

[154] *REGULATION (EC) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Law Applicable to Contractual Obligations (Rome I)*.
[155] Bradshaw, Millard, and Walden, "Contracts for Clouds," 198–200.
[156] *Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters*.

user. The question is whether the EU law will apply as the activities were conducted in the context of EU service provider's establishment? The answer can be affirmative based on article 4(1) a of the EU directive.

Legal literature obviates, that when processing non-EU citizen's data certain gaps might arise with regard to the applicable law matters. For instance, when it comes to the service provider not established in EU territory who processing data in the context of the activities. Article 4 (1) a, would not apply because company has no establishment on the EU territory. It was highlighted that processing took place in the context of activities with suggesting service in non-EU territory.[157] However, inconsistency is appeared among two statement described in the theory. It is expressed that article 4 (1) c does not apply as well. If the reason for the first case was non-EU establishment, in the second example it is considered that activities were in the context of EU establishment.[158] That was the reason that article 4 (1) c does not apply and ambiguity of the law appeared. Although, Article 29 working party considered that here should be no gap, because there is not "relevant" establishment at this case and EU establishment should not be counted. [159]

However, when it comes to cloud computing where Article 4 (1) a is applicable, application of Article 4 (1) c is excluded. But in case, when controller is established in EU territory and is using the equipment of the EU establishment, article 4 (1) a will apply, because the controller's establishment place and context of activities is decisive element and the last one – establishment of the equipment.[160]

The court cases coincides my argumentation while considering activities in EU establishment. I will discuss two cases and both of them have deal with applicable law in cloud computing

[157] Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 13–14. Moerel, "The Long Arm of EU Data Protection Law," 8.
[158] Ibid
[159] "Article 29 Data Protection Working Party, WP 179," 29.
[160] Ibid., 30–31.

services: first one is Google v. Italy case and the second one is recent decision from the 2013 year, Google v. Spain case.

European court of Justice (ECJ) in Google v. Italy assessed whether processing of the data was conducted in the context of EU establishment. According to the facts of the case, main office of Google Inc. was considered to be the US establishment. Also ECJ considered users as the data controllers in cloud computing. However, Google Italy was the "operative and commercial hand' of Google Inc."[161]

It is interesting that company's servers where located in US and processing took place in US, while Ireland office controlled the content of the data processing. Although, AdWords used by Google were governed by Google Italy office. The court made decision in favor of Italian law and the major factor which played important role was the processing operation and it took place under the Italian office, because videos, content of processing was uploaded under Italian jurisdiction.[162]

This decision can be criticized due to the fact that ECJ tried to extend EU jurisdiction on the case, where processing of the data was not conducted on the EU territory but was performed in US establishment.[163] Although equipment was located on EU territory court could not justify the existence of the EU establishment[164], thus Articles 4(1) c and 4 (1) a were not applicable.

The above analyses demonstrate that it is difficult to determine who has effective control on data content. Cloud clients were considered as a controller of the data, but at the same time service providers were deemed to have effective control on hardware and software of the data.

[161] Sartor and Viola de Azevedo Cunha, "The Italian Google-Case," 8.
[162] Ibid.Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 9–10.
[163]Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 9–10.
[164] Mantelero, "Cloud Computing, Trans-Border Data Flows and the European Directive 95/46/EC: Applicable Law and Task Distribution," 1.

There is no indication in the decision that controller's establishment place was determinative ground to the court while ruling on the case. As already stated above, the decisive factor was context of the activities carried out by Italian establishment. The processing operation was performed by the Italian established service provider.

Similarly, in Google v. Spain case, Spain was branch office of Google Inc. The main factor why court ruled that Spanish law was applicable was due to the commercial activity of the branch.[165] The substantial reason defining applicable law was business activity of the company in Spanish established service provider. Court evaluated that processing was held by the Spanish established service provider, therefore the processing activities were considered to be carried out by EU establishment.[166]

The court decisions demonstrated that activities of service provider are decisive factor in deciding applicable law. Court does not consider service provider as a data controller. However, the role of the user, in these cases, as a data controller is minimum. Moreover, user is considered to be a data controller in cloud computing services. This might be confusing when the court decides case considering the activities performed by service provider. In on this way court extends the definition of article 4 (1) a . In the end the scope of EU directive broadened, covers not only EU established companies, but non-EU established ones as it was decided in the abovementioned cases. Court practice is important source for identifying who handles the processing of the data and inconsistent decisions may threaten uniform interpretation of the Directive. The above court decision has in fact been criticized for the inconsistency with previous practice on interpretation of the Directive, which creates discrepancies on choice of law issues. The result of the said statements could be the extended interpretation of the data protection directive and globalization of law provisions, regardless the fact that controller/user has EU establishment or not.

[165] Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González ; OPINION OF ADVOCATE GENERAL JÄÄSKINEN, para 62 (ECJ 2013), para 62.
[166] Ibid., para 66.

New data protection regulation is worth mentioning here, particularly with regard to the issues of applicable law and choice of forum. Article 3 of the regulation represents one-stop-shop forum, which considers that EU law applies if non-EU established company *"offering of goods or services to such data subjects in the Union"*; The said provision may increase the influence of EU forum. Theoretically almost every company, who offers goods and service in Europe would be under the scope of the EU regulation. As a result, non-EU established companies would avoid EU market.[167] However, EDPS is against amendment on the regulation as well. EDPS considers that the new provision will cover all the companies, irrespective of place of residence, the regulation will become worldwide and can be misleading for the business.[168] The question of applicable law would still remain unresolved. The new regulation attempts to extend the territorial scope of European regulation to make it impossible to avoid EU data protection law. However, the result would be contrary, ambiguity in the law and negative effects on business.

3.3.2 Data Location Factor in Using Equipment

Apart from the general requirements for defining applicable law in cloud computing cases data location plays significant factor as well. The location of user's data may be changed easily according to the geographic location, in EU and outside EU territory.[169] The said statement can have effect defining choice of law in cloud computing service.[170] The first example regarding the flow of data from one country to another and defining data location problem can be provided based on Article 4 (1) c of EU Directive, when equipment is used

[167] Omer and Wolf, "White Paper Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation," 8.
[168] "Additional EDPS Comments on the Data Protection Reform Package," 5.
[169] Hon and Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4," 6.
[170] "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe,'" 6.

for the processing data, such as using cookies. Point of interest is also the issue of changing data location within the EU borders. The practical aspects of this matter can be demonstrated on the example of the cookies.

Cookie is *"text files, neither software, spyware, nor viruses which are 'set', saved onto a user's computing equipment by the user's web browser, when the user visits a webpage with the browser and the browser automatically follows instructions sent by the web server to save the cookie"*.[171] "*Cookies merely consist of data and allow for the exchange of information of user's computer and the website that placed the cookie*".[172]

Also in cloud computing scenario may arise situation when service provider is processing data using software program\equipment or processing data using cookies, will they considered as the same. We have mentioned that using equipment is the same as using cookies, but is it equalized to the user's ability using service provider's infrastructure, software program, to process data in online contracts. From the abovementioned text definition of cookies and using equipment in electronic contracts may not be the same. Cookies is one type of equipment in cloud computing. Although, from the consequence side, there should be the same result, EU law can be applicable in both cases, article 4 (1) c.

Furthermore, the issue of effective control on data location is directly connected to the obligation of controller, who is in charge of processing data in the internet. Controller, itself plays substantial factor in defining applicable law.

Generally, in case of cloud computing services, applicable is the country where controller's cloud computing services are established, not the place in which the cloud computing providers are located.[173] This provision comes from the statement as we were discussing before, in chapter 2.1.1., 2.1.2. defining controller, processor in cloud computing. Such as cloud computing service provider is the processor and the user/customer is the controller of

[171] "Article 29 Data Protection Working Party, WP 56," 10.
[172] Moerel, "The Long Arm of EU Data Protection Law," 12.
[173] "Article 29 Data Protection Working Party, WP 196," 7.

the data. This means that service provider's place plays not active role in processing information, just fulfills the directive of the controller/user. The determinative factor here as well is the activities in the context of processing which took place in time of uploading data in clouds. [174]

In case of cookies the picture is different. Significant factor is that, when service provider runs cookies it is considered to be using equipment and therefore according to Article 4 (1) (c) application of EU law is triggered.[175] This assertion leads to the conclusion that the service providers are the data controllers for the purposes of cookies. The management of the data location is up to the service provider, who stores and keeps the data with the permission of the user.[176] However, the argument is often advanced that only SaaS service provider could be considered as a controller of the data with respect to cookies.[177]

The European Court of Justice has made rather controversial decision regarding the influence of parties in data location cloud computing scenario in the case of Bodil Lindqvist case.[178] Ms. Bodil uploaded data about her colleges in social network, which has been qualified as uploading data to the cloud computing server.[179] The reasoning of the ECJ can be summarized as follows: information on internet is easily uploaded by the indefinite number of people.[180]At the same time infrastructure on internet is located in one or more countries and for the service provider it is difficult to control the data location.[181] Controversially, court considered that service provider in the internet could not be a controller of the data and left the responsibility to the users on data location issues.

---

[174]see chapter 3.2.2
[175] "Article 29 Data Protection Working Party, WP 179," 21.
[176] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*, article 5 (1).
[177] Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 17.
[178] Criminal proceedings against Bodil Lindqvist (European Court of Justice 2003).
[179] "Article 29 Data Protection Working Party, WP 163," 5.
[180] Criminal proceedings against Bodil Lindqvist, para 58 (European Court of Justice 2003), para 58.
[181] Ibid., para 59.

Controversies regarding controlling data location in the internet trigger problems in defining applicable law. If we assume that using devices (computer) could be considered as using equipment, user's computer can be viewed as equipment with respect to cookies if it is outside EU territory.[182] This is important when determining applicable law. As discussed in the previous chapter controller/user could own equipment\computer. At the same time, if the user is considered to be a controller of the data, then it appears that computer, user outside EU territory, collects data of EU citizens. This does not trigger application of the EU law in every case, since the user/controller may not have the EU establishment in which case Article 4 (1) (a) of the Directive will not be applied. Likewise, Article 4 (1) (c) of the Directive will not be applicable either, since the equipment\computer is located in another country. This may create the problem in reality, as the application of the EU law will be avoided altogether. It seems that the Directive provisions are too broad and not entirely cut out to fit the reality. The data belonging to the EU citizens may be processed to the other country as exemplified above without triggering application of EU data protection rules.

The way out of situation for the protecting EU citizen's data could be reminding companies article 25 and 26 of data protection directive for the adequate protection of EU citizen's data, while data flows to the third country. To my mind the problem here could be that it is hard in every contract to require party adequate level of protection, that's why theoretically first step is more relevant. EU directive broadened choice of law requirements and become EU law applicable for not EU established companies. The first step usually is more relevant, then the second one. Another case could be that I will remind the assertion of former chapter 2.2.1. Such as using another parties infrastructure may be considered as using yours. So at this case, service provider could use the user computer as infrastructure and control the location of the data.

Another example of avoiding applicability of the EU law could be US based company, which sells goods and provides service in the US. If the company uses cookies in EU territory without any EU establishment and offers advertisement in the EU territory without selling

[182] "Article 29 Data Protection Working Party, WP 56," 10. Kuner, *European Data Protection Law*, 118.

goods, application of EU law can not be triggered. The conditions of using equipment in the EU territory such as suggesting advertisement using cookies, does not mean that Article 4 (1) (c) of the Directive will apply. Company has no business activity within the EU and has no reason to process data. The company is using cookies with the sole aim to collect information as opposed to identification purposes.[183] According to this example one can distinguish between two different objectives of using equipment, one being the collection of the data and the other - an advertisement.

It is appeared that in practice we have the problem applying EU law on non-EU based websites if they are collecting data from the European Union. The main idea of the article 4 (1) c of EU directive is that the processing, with using equipment should have the purpose of process data. The purpose exists while the company is doing business in EU territory. If company is not doing business it has no influence in EU territory and for this reasons article 4 (1) c does not apply. At the same time company collects the data of EU citizens, such as example of advertisement I represented, directive does not apply according to the mentioned directive article. So this is the point, EU law seems broad from one side but in practice it is not applying. That's why it is recommended that the articles about the applicable law were more precise to have less holes in practice.

Another example of using equipment which effects on data location could be data centers. If the data center using equipment, for the processing data, it could be argued that, equipment makes establishment place of the data center[184]. On the other hand it could be considered that data center does not facilitate activities on its own and the activities could not be in a context of the processing[185]. Data centers can make technical support of the controller to process data and could not cause any profit for the data security or processing measure and could not be considered as a relevant establishment.

[183] Moerel, "The Long Arm of EU Data Protection Law," 12–13.
[184] Hon, Millard, and Julia, "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," 18–19.
[185] Ibid.

The conclusion from the said assertion could be that if we consider that the used equipment is not the place of the establishment and article 4.1.c. does not apply, at the same time it could be considered that the same establishment is not in the context of the activities according to the article 4 1 a, because as we mentioned, it is not a relevant establishment.

This may cause problems on deciding applicable law, because cloud computing server may use data center for flow of data from one country to another, outside EU area as well. As we consider users as data controllers, in such situation, it becomes hard for them to control the data location, for the reason lack of technical equipment. This causes problem to define the applicable law in non-EU or EU established companies. However, establishment place of server will not be taken into consideration for deciding applicable law.[186] Also, as the data may be flow in EU or outside EU and the location of the data will be unknown, it would be hard to decide if the processing procedure was in the context of EU establishment.

The legal dispute concerning the actions of non-EU established cloud service provider, who rents the space or/and uses equipment, may be subject of the EU jurisdiction. Provided that the data is transferred from the EU, regardless of the fact that collecting of such data took place outside the EU and the said data does not belong to the EU citizens. At the same time, if controller has EU establishment and transfers data to the third country EU law applies. This may create problems of enforceability of the EU laws in practice and may have result that companies with non-EU establishment may refuse to offer services within the EU territory.[187]

To sum up, provisions of the Directive concerning the forum in cloud computing service are not entirely straightforward. Arguably, they fail to operate in a manner overcoming the difficulties of the applicability so often raised in practice. In case of service provider/websites using cookies and processing non-EU citizens' data, the EU law should be applicable. The same applies to non-EU established controller/user, using service provider's infrastructure. However, in the

[186] Hon and Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4," 6–7.
[187] Ibid., 8.

former case Article 4 (1) (a) of the Directive shall apply, whereas in the latter case application of Article 4 (1) (c) of the Directive will be triggered.

4 conclusion

In the thesis I have showed how it is defined applicable law in EU established companies/service providers, what difficulties may arise in practice. Answering the thesis question, first of all, I have interpreted electronic contract and concluded that contract between service provider and the user is the electronic contract. I have highlighted that in electronic contract the main parties are business as cloud computing service provider and the user. The research evaluates that role of the user and the service provider in electronic contract defines if company's action falls under EU jurisdiction or not. In the electronic contracts users were considered as the controller of the data and service provider as the processor of the data.

However, assertion has counterarguments in practice. Such as it was the question how user could fulfill obligation set by the directive and regulation. That's why it was recommended to consider the user as the data subject. Although, contractual provision, define user as a controller and service provider processor does not mean that user will not be considered as a processor in some processing operations. In the end research gave the conclusion that examples from the practice showed that case by case should be decided the functions of the parties in the contract more precisely. However, this provision does not exclude the said statement that mostly, in theory users are controller and service providers are processor in cloud computing service.

In the thesis it was evaluated that service provider is using public cloud in electronic contracts, which creates obscurities on defining law. Significant factor is that data location may be changed easily in cloud service. User as a data controller should investigate where the processing operation was fulfilled. The thesis showed that it is difficult to consider where data was located when non-EU established company processes data in EU territory using equipment, such as cookies, data centers. Another factor could be processing operation in the context of EU establishment. The case study showed that service provider's establishment

place was major factor for defining the applicable law, not the controller's establishment place. In the end the law regulation and interpretation of the court showed that the EU directive provisions on applicable law and in controller, processor is general. This gives the possibility of the court interpret case and cover non-EU established companies in EU establishment if they process data in EU territory. All in all the main reason of general provisions in data protection directive and regulation is that EU legislators aim to extend territorial scope of data protection for avoid misuse of European citizens' data.

Reference

Legislations

"Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce')." Official Journal L 178 , 17/07/2000 P. 0001 - 0016, n.d.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), n.d. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT.

"Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." Official Journal L 281 , 23/11/1995 P. 0031 - 0050, n.d.

"Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts - Statement by the Council and the Parliament Re Article 6 (1) - Statement by the Commission Re Article 3 (1), First Indent." Official Journal L 144 , 04/06/1997 P. 0019 - 0027, n.d. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:en:HTML.

Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 2000. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:EN:NOT.

REGULATION (EC) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Law Applicable to Contractual Obligations (Rome I). No 593/2008, 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:177:0006:0006:en:PDF.

"Proposal for a Regulation of the European Parliament and of the Council- on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)." COM(2012) 11 final 2012/0011 (COD) C7-0025/12, October 21, 2013.

http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131021_1830.htm.

Other EU documents

"2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce (notified under Document Number C(2000) 2441) (Text with EEA Relevance.)," n.d. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

"Additional EDPS Comments on the Data Protection Reform Package," March 15, 2013. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

"Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions 'Unleashing the Potential of Cloud Computing in Europe.'" Brussels, 27.9.2012 COM(2012) 529 final, September 27, 2012. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

Digital Single Market Group. "Position Paper on the Proposed General Regulation on Data Protection," March 2013. http://dpalliance.org.uk/; http://dpalliance.org.uk/wp-content/uploads/2013/03/1303_Data-Protection-Position-Paper2.pdf.

EUROPEAN COMMISSION. *Cloud Computing: Public Consultation Report*. Brussels: Information Society and Media Directorate-General Converged Networks and Services Software & Service Architectures and Infrastructures, December 5, 2011.

Final report to the Information Commissioner's Office. *Implications of the European Commission's Proposal for a General Data Protection Regulation for Business*, May 2013. http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Research_and_reports/implications-european-commissions-proposal-general-data-protection-regulation-for-business.ashx

Omer, Tene, and Christopher Wolf. "White Paper Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation." The Future of Privacy Forum, January 2013.

"Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe,'" November 16, 2012. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

Peter, Hustinx, European Data Protection Supervisor. "Panel IV: Privacy and Cloud Computing 'Data Protection and Cloud Computing under EU Law.'" presented at the Third European Cyber Security Awareness Day, BSA, European Parliament,, April 13, 2010. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf.

Article 29 Working Documents

"Article 29 Data Protection Working Party 'Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites' WP 56," May 30, 2002.

"Article 29 Data Protection Working Party 'Opinion 05/2012 on Cloud Computing' WP 196," July 1, 2012.

"Article 29 Data Protection Working Party 'Opinion 1/2010 on the Concepts of 'Controller' and 'Processor WP 169," February 16, 2010.

"Article 29 Data Protection Working Party 'Opinion 4/2007 on the Concept of Personal data'WP 136," June 20, 2007.

"Article 29 Data Protection Working Party 'Opinion 5/2009 on Online Social Networking' WP 163," June 12, 2009.

"Article 29 Data Protection Working Party 'Opinion 8/2010 on Applicable Law'; WP179," December 16, 2010.

"Article 29 Data Protection Working Party; Working Party on Police and Justice 'The Future of Privacy Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' WP 168," December 1, 2009.

"Article29 Data Protection Working Party 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' WP128," November 22, 2006.

Books

Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic, and Limits*. Information Law Series 10. The Hague ; New York: Kluwer Law International, 2002

Kuner, Christopher *Law and the Internet*. 3rd ed. Oxford [England] ; Portland, Or: Hart Pub, 2009.

Kuner, Christopher. *European Data Protection Law: Corporate Compliance and Regulation*. 2nd ed. Oxford ; New York: Oxford University Press, 2007.

Lessig, Lawrence. *Code: Version 2.0*. 2nd ed. New York: Basic Books, 2006.

Davidson, Alan. *The Law of Electronic Commerce*. Port Melbourne, Vic: Cambridge University Press, 2009

Svantesson, Dan Jerker B. *Private International Law and the Internet*. 2nd ed. Alphen aan den Rijn : Frederick, MD: Kluwer Law International ; Sold and distributed in North, Central and South America by Aspen Publishers, 2012.

Gutwirth, Serge. *Computers, Privacy and Data Protection an Element of Choice*. Dordrecht; New York: Springer, 2011. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=371200

Articles

Bender, Scott. "Privacy in the Cloud Fronter: Abandoning the 'Take It or Leave It' Approach." *Drexel Law Review* (521 487AD). http://earlemacklaw.drexel.edu/~/media/Files/law/law%20review/spring_2012/Bender.ashx.

Boss, Amelia H. "IV. Electronic Contracting: Legal Problem or Legal Solution?" United Nations, New York, 2004, n.d. http://www.unescap.org/publications/detail.asp?id=1028.

Bradshaw, S., C. Millard, and I. Walden. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." *International Journal of Law and Information Technology* 19, no. 3 (July 20, 2011): 187–223. doi:10.1093/ijlit/ear005.

Bygrave, Lee A "Determining Applicable Law pursuant to European Data Protection Legislation." *Computer Law & Security Report, 2000,* volume 16 (n.d.): 252–257.

Chalton, Simon. "The Court of Appeal's Interpretation of 'Personal Data' in Durant v. FSA - a Welcome Clarification, or a Cat amongst the Data Protection Pigeons?" *Computer Law & Security Report, 20004* Vol 20 no.3 2004 (n.d.): 175–181.

Froomkin, A. Michael. "Almost Free: An Analysis of ICANN's 'Affirmation of Commitments.'" *Journal of Telecommunications and High Technology Law,* Vol. 9, 2011 (January 20, 2011). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1744086..

Hon, W Kuan, and Christopher Millard. "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4." *Queen Mary School of Law Legal Studies Research Paper No. 85/2011* Vol. 9:1, No. 25 (April 4, 2012). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925066.

Hon, W Kuan, Christopher Millard, and Hörnle Julia. "Data Protection Jurisdiction and Cloud Computing – When Are Cloud Users and Providers Subject to EU Data

Protection Law? The Cloud of Unknowing, Part 3." *International Review of Law, Computers & Technology;* Vol. 26, No. 2–3, 2012 (February 9, 2012). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240&rec=1&srcabs=2034286&alg=1&pos=1.

Hon, W Kuan, Christopher Millard, and Ian Walden. "Negotiating Cloud Contracts: Looking at Clouds from the Both Side Now." *Stanford Technology Law Review* Volume 16, number 1 fall 2012 (n.d.): 79–129. Accessed October 21, 2013.

———. "Who Is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2." *International Data Privacy Law (2012)* 2 (1): 3–18 (March 21, 2011). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130&rec=1&srcabs=1924240&alg=1&pos=1.

Kuner, C. "Data Protection Law and International Jurisdiction on the Internet (Part 2)." *International Journal of Law and Information Technology* 18, no. 3 (March 11, 2010): 227–247. doi:10.1093/ijlit/eaq004.

———. "Data Protection Law and International Jurisdiction on the Internet(Part 1)." *International Journal of Law and Information Technology* 18, no. 2 (March 11, 2010): 176–193. doi:10.1093/ijlit/eaq002.

Kuner, Christopher.*Regulation of Transborder Data Flows under Data Protection and Privacy Law Past, Present and Future*, December 8, 2011. http://www.oecd-ilibrary.org/science-and-technology/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_5kg0s2fk315f-en.

———. "Submission to the 'Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union'" (January 14, 2011). http://ec.europa.eu/justice/news/consulting_public/0006/contributions/citizens/kuner_christopher_en.pdf.

Mantelero, Alessandro. "Cloud Computing, Trans-Border Data Flows and the European Directive 95/46/EC: Applicable Law and Task Distribution." *European Journal of Law and Technology* Vol. 3, No. 2 (2012). http://ejlt.org/article/viewFile/96/254.

Moerel, L. "Back to Basics: When Does EU Data Protection Law Apply?" *International Data Privacy Law* 1, no. 2 (January 24, 2011): 92–110. doi:10.1093/idpl/ipq009.

———. "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?" *International Data Privacy Law* 1, no. 1 (November 2, 2010): 1–19. doi:10.1093/idpl/ipq004.

Poullet, Yves. “EU Data Protection Policy. The Directive 95/46/EC: Ten Years after.” *Computer Law & Security Review* 22, no. 3 (January 2006): 206–217. doi:10.1016/j.clsr.2006.03.004.

Ramberg, C.H. “The E-Commerce Directive and Formation of Contract in a Comparative Perspective.” *Global Jurist Advances* Vol. 1, Issue 2 (2001), Article 3 (n.d.). http://www.bepress.com/cgi/viewcontent.cgi?article=1023&context=gj.

Sartor, G., and M. Viola de Azevedo Cunha. “The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents.” *International Journal of Law and Information Technology* 18, no. 4 (August 25, 2010): 356–378. doi:10.1093/ijlit/eaq010.

.

Weitzenboeck, Emily. “Electronic Agents and the Formation of Contracts.” *International Journal of Law and Information Technology* Vol. 9, Issue 3, Autumn 2001, (n.d.). http://folk.uio.no/emilyw/publications/.

Winn, J.K. & Haubold, J. “Electronic Promises: Contract Law Reform and E-Commerce in a Comparative Perspective.” *European Law Review (2002)* Vol. 27, Issue: 5 (n.d.). http://www.law.washington.edu/Directory/docs/Winn/Electronic_Promises_Revised.pdf.

Wong, Rebecca. “Data Protection: The Future of Privacy.” *Computer Law & Security Review* 27, no. 1 (February 2011): 53–57. doi:10.1016/j.clsr.2010.11.004.

Zimmeck, Sebastian. “The Information Privacy Law of Web Applications and Cloud Computing.” *Santa Clara Computer & High Technology Law Journal* Volume 29, Issue 3 Article 1 (April 23, 2013): 451–487.

PHD thesis

Nuth, Maryke Silalahi. “E-Commerce Contracting: The Effective Formation of Online Contracts.” Dissertation for the degree of PhD 2010, University of Oslo, Faculty of Law, n.d.

Cases

ARO Lease BV v Inspecteur van de Belastingdienst Grote Ondernemingen te Amsterdam (European Court of Justice 1997). Case C-190/95

Criminal proceedings against Bodil Lindqvist (European Court of Justice 2003). Case C-101/01

The Queen v Secretary of State for Transport (European Court of Justice 1991) Case C-221/89.

College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer (European Court of Justice 2009). Case C-553/07

Gatton v. T-Mobile USA, Inc., the California Court of Appeals 61 Cal. Rptr. 3d 344, 356–58 (Cal. Ct. App. 2007), cert. denied, 553 U.S. 1067 (2008). (n.d.).

Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González ; OPINION OF ADVOCATE GENERAL JÄÄSKINEN (ECJ 2013). Case C 131/12

Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt (European Court of Justice 1985) Case 168/84

Somafer SA v Saar-Ferngas AG (European Court of Justice 1978). Case 33/78

Blanckaert & Willems PVBA v Luise Trost (European Court of Justice 1981). Case 139/80

Websites:

http://www.booking.com/general.en-gb.html?dcid=1&lang=en gb&sid=ecabfd4cd95f5afa3f2080bd637e9437&tmpl=docs%2Fterms-and-conditions;

http://www.hostelworld.com/hosteltermsandconditions.php

http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131021_1830.htm

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

http://europa.eu/about-eu/institutions-bodies/edps/

http://www.privacycommission.be/